DEPARTMENT OF THE ARMY
HEADQUARTERS, US ARMY ARMOR CENTER AND FORT KNOX
75 6TH AVENUE
FORT KNOX, KENTUCKY 40121-5717

REPLY TO
ATTENTION OF:

Expires 14 July 2008

IMSE-KNX-IMA (25)

14 July 2006

MEMORANDUM FOR

Commanders, All Units Reporting Directly to This Headquarters
Commanders, Fort Knox Partners In Excellence
Directors and Chiefs, Staff Offices/Departments, This Headquarters

SUBJECT: Fort Knox Policy Memo No. 39-06 – Information Assurance (IA) Policy and Electronic Mail (E-mail) Privacy and Usage

1. References.

a. DODI 5200.40, DOD Information Technology Security Certification and Accreditation Process (DITSCAP), 30 December 1997.

b. DOD Chief Information Officer (CIO) Guidance and Policy Memorandum No. 8-8001, 31 March 2000, subject: Global Information Grid.

c. DOD CIO G&PM No. 6-8510, 16 June 2000, subject: Department of Defense Global Information Grid Information Assurance.

d. DOD CIO G&PM No. 4-8460, 24 August 2000, subject: Department of Defense Global Information Grid Networks.

e. DOD CIO G&PM No. 10-8460, 24 August 2000, subject: Network Operations.

f. DODD 8500.1, Information Assurance (IA), 24 October 2002.

g. DODI 8500.2, Information Assurance (IA) Implementation, 6 February 2003.

h. AR 25-2, Information Assurance, 14 November 2003.

i. AR-25-1, Army Knowledge Management and Information Technology, 15 July 2005.

2. Purpose. The Fort Knox Directorate of Information Management (DOIM) e-mail system is the primary command and control system for general operational and administrative issues and provides a vehicle for communicating electronically with external resources. It provides a reliable; timely; and direct method of exchanging information, sharing ideas, and eliciting responses. This policy identifies and eliminates potential entries into the campus area network (CAN) that bypasses boundary security protection and details what activities are prohibited and permitted.

3. Applicability. This policy applies to all Soldiers, civilians, and contractors who use e-mail on any computer system connected to the Fort Knox CAN.

4. Responsibilities.

a. Commanders, directors, and supervisors at all levels shall ensure that subordinate personnel are aware of permissible and unauthorized use of Government e-mail resources and understand that inappropriate use may be a basis for disciplinary action.

b. E-mail users shall use e-mail resources responsibly and abide by normal standards of professional and personal conduct at all times.

c. The DOIM Information Assurance Manager (IAM) shall ensure that all e-mail users are familiar with the policies and procedures contained herein. Possible criminal activity shall be reported to the DOIM IAM immediately for assessment and appropriate action. When illegal activity is confirmed, the commander/director shall be notified by the DOIM IAM.

d. E-mail Privacy Policy and Monitoring of Computer Usage.

(1) No Expectation of Privacy. The computers and computer accounts given to personnel assists them in performance of their jobs, and they should not have an expectation of privacy in anything they create, store, send, or receive on the computer system.

(2) No Privacy in Communications. Personnel should never consider electronic communications to be private. Remember that when you send an e-mail message, others may forward it to individuals without your knowledge. With that in mind, you should know that e-mails you send may be stored indefinitely on any number of computers. In addition, e-mail sent to nonexistent or incorrect usernames may be delivered to unintended recipients.

(3) Prohibited Activities. Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate may not be sent by e-mail. Personnel encountering or receiving this kind of material should follow the reporting requirements detailed in paragraph 6 of this policy.

(4) Viruses. Viruses can cause considerable damage to computer systems. Users should never download or accept e-mail attachments from unknown senders or use media from outside sources without first scanning the material with the Symantec Anti-virus or an Army-approved virus checking software. If users suspect that a virus has been introduced into the Government's network, they should notify their Information Assurance Security Officer (IASO), Information Management Officer (IMO), or the DOIM Customer Support Center immediately to obtain advice on the next course of action.

5. E-mail Policy of Computer Usage.

a. Usage.

(1) Government computer e-mail use for personal matters is authorized within certain limitations: personal use must not adversely affect the performance of official duties, is made during the employee's personal time, does not reflect adversely on the Federal Government, does not overburden the communication system, and does not create any additional cost to DOD. E-mail is unclassified official business and is used in the interest of the Government.

(2) **For Official Use Only (FOUO), Privacy Act, and military operational information must be sent encrypted.**

b. Limitations. DOIM provides each user with an e-mail account with a standard mailbox size of 75 MB. The e-mail system setup automatically notifies users when the following thresholds are reached:

(1) Issue Warning. 60 MB.

(2) Prohibit Send. 70 MB (user will not be able to send messages if this threshold is reached).

(3) Prohibit Send and Receive. 75 MB or when the mailbox limit has been exceeded; user will not be able to send or receive messages if this threshold is reached.

c. Mailbox responsibility. The user is responsible for normal mailbox maintenance (includes mailbox size management, purging deleted items, moving mail to a personal folder (.pst file), etc.).

d. Prohibited Use. E-mail systems will not be used for purposes that could reasonably be expected to cause, directly or indirectly, congestions, delays, or disruptions of service to any computing facilities or unwarranted or unsolicited interference with others' use of e-mail. Such prohibited use includes but is not limited to:

(1) Creating; downloading; storing; transmitting; or broadcasting chain letters, jokes, and unofficial pictures.

(2) "Spam" used to exploit list servers or similar broadcast systems for purposes beyond their intended scope, which amplifies the wide spread distribution of unsolicited e-mail.

(3) Broadcasting unsubstantiated virus warnings from sources other than the DOIM IA office.

(4) Broadcasting e-mail messages to large groups of e-mail users (entire organizations) instead of targeting smaller populations.

(5) Unlawful activities; commercial purposes; or support of "for profit" activities, personal financial gain, personal use inconsistent with DOD policy, and use that violates other Army policies or public laws.

(6) If classified documents are received via e-mail, the user must immediately notify the IASO/IMO, activity security manager, and the DOIM IAM. Classified information on unclassified machines is a security violation and must be reported immediately for appropriate action.

(7) Forwarding Official Government e-mail to an ISP account and/or forwarding e-mail from an ISP account to a Government e-mail account.

(8) Configuring Government e-mail accounts to automatically forward to a personal ISP account or vice versa.

6. Reporting Inappropriate Activity. Users shall submit complaints about inappropriate internet or e-mail activity to their IASO or IMO. The IASO/IMO informs the DOIM IAM. The DOIM IAM will review the inappropriate activity and determine appropriate action to be taken (i.e., notify the user's commander, notify Regional Computer Emergency Response Team, etc.).

7. Prohibited activities discovered during routine security monitoring, systems administrator review, or other authorized oversight activities shall be turned over to the appropriate authorities for investigation. Government personnel who use the internet or e-mail for prohibited activities are subject to disciplinary action in accordance with Office of Personnel Management or Uniform Code of Military Justice guidelines. Contractor personnel using Government systems to access the internet for prohibited activities shall be handled through contract channels.

FOR THE COMMANDER:

MARK D. NEEDHAM
COL, AR
Garrison Commander

DISTRIBUTION:
A